

# Cyclicity degrees of finite groups

Marius Tărnăuceanu, László Tóth

Acta Math. Hungar. **145** (2015), 489–504

## Abstract

We introduce and study the concept of cyclicity degree of a finite group  $G$ . This quantity measures the probability of a random subgroup of  $G$  to be cyclic. Explicit formulas are obtained for some particular classes of finite groups. An asymptotic formula and minimality/maximality results on cyclicity degrees are also inferred.

**MSC (2010):** Primary 20D60, 20P05; Secondary 20D30, 20F16, 20F18.

**Key words:** cyclicity degree, subgroup lattice, poset of cyclic subgroups, number of subgroups.

## 1 Introduction

In the last years there has been a growing interest in the use of probability in finite group theory. One of the most important aspects which have been studied is the probability that two elements of a finite group  $G$  commute. It is called the *commutativity degree* of  $G$ , and has been investigated in many papers, as [3, 8, 9, 10, 11, 12, 14, 16]. Inspired by this concept, in [21] the first author introduced a similar notion for the subgroups of  $G$ , called the *subgroup commutativity degree* of  $G$ . This quantity is defined by

$$\begin{aligned} \text{sd}(G) &= \frac{1}{|L(G)|^2} |\{(H, K) \in L(G)^2 : HK = KH\}| = \\ &= \frac{1}{|L(G)|^2} |\{(H, K) \in L(G)^2 : HK \in L(G)\}| \end{aligned}$$

(where  $L(G)$  denotes the subgroup lattice of  $G$ ) and it measures the probability that two subgroups of  $G$  commute, or equivalently the probability that

the product of two subgroups of  $G$  be a subgroup of  $G$  (recall also the natural generalization of  $\text{sd}(G)$ , namely the *relative subgroup commutativity degree* of a subgroup of  $G$ , introduced and studied in [23]).

Another probabilistic notion on  $L(G)$  has been investigated in [25]: the *normality degree* of  $G$ . It is defined by

$$\text{ndeg}(G) = \frac{|N(G)|}{|L(G)|}$$

(where  $N(G)$  denotes the normal subgroup lattice of  $G$ ) and measures the probability of a random subgroup of  $G$  to be normal.

Clearly, analogous constructions can be made by replacing  $N(G)$  with other remarkable posets of subgroups of  $G$ . One of them is the poset of cyclic subgroups of  $G$ , usually denoted by  $C(G)$ . In this way, one obtains the following quantity

$$\text{cdeg}(G) = \frac{|C(G)|}{|L(G)|},$$

that measures the probability of a random subgroup of  $G$  to be cyclic and will be called the *cyclicity degree* of  $G$ . Its study is the main purpose of our paper.

Note that for an arbitrary finite group  $G$  computing the number of subgroups, as well as the number of cyclic subgroups, is a difficult work. These numbers are in general unknown, excepting for few particular classes of finite groups. We also recall the powerful connection between the cyclic subgroup structure of a finite group and the set of its element orders.

The paper is organized as follows. Some basic properties and results on cyclicity degree are presented in Section 2. Section 3 deals with cyclicity degrees for some special classes of finite groups: abelian groups, hamiltonian groups,  $p$ -groups possessing a cyclic maximal subgroup and ZM-groups. An asymptotic formula for  $\sum_{n \leq x} \text{cdeg}(\mathbb{Z}_n \times \mathbb{Z}_n)$  is also deduced. In Section 4 we give several minimality/maximality results and conjectures on cyclicity degrees of finite abelian  $p$ -groups. In the final section an problem is formulated.

Most of our notation is standard and will usually not be repeated here. Elementary notions and results on lattices (respectively on groups) can be

found in [2] (respectively in [6, 7, 17]). For subgroup lattice concepts we refer the reader to [15, 18, 19].

## 2 Basic properties of cyclicity degree

Let  $G$  be a finite group. First of all, remark that the cyclicity degree  $\text{cdeg}(G)$  satisfies the following relation

$$0 < \text{cdeg}(G) \leq 1.$$

Moreover, we have  $\text{cdeg}(G) = 1$  if and only if  $G$  is cyclic.

Next we observe that several finite non-cyclic groups, as  $S_3$ , satisfy the property that all their proper subgroups are cyclic. We are able to determine all finite groups satisfying this property.

**Theorem 2.1.** *Let  $G$  be a finite group. Then*

$$\text{cdeg}(G) = \frac{|L(G)| - 1}{|L(G)|}$$

*if and only if  $G$  is either a certain semidirect product of a normal subgroup of order  $p$  by a cyclic subgroup of order  $q^n$  ( $p, q$  primes,  $n \in \mathbb{N}^* := \{1, 2, \dots\}$ ), an elementary abelian  $p$ -group of rank two or the quaternion group  $Q_8$ .*

*Proof.* Let  $G$  be a finite non-cyclic group all of whose proper subgroups are cyclic.

Case I. Assume that  $G$  is not a  $p$ -group. Since  $G$  is not cyclic and all its Sylow subgroups are cyclic, we infer that there is a Sylow  $q$ -subgroup  $S \cong \mathbb{Z}_{q^n}$  which is not normal. Then  $N_G(S)$  is different from  $G$  and consequently it is cyclic by our hypothesis. It follows that  $S$  is contained in  $Z(N_G(S)) = N_G(S)$ . By the Burnside normal  $p$ -complement theorem (see [7, Th. 5.13]) we obtain that  $G$  has a normal  $q$ -complement  $T$  (note that  $T$  is also cyclic). Then  $TS = G$ , i.e.,  $G$  is a semidirect product of a cyclic normal subgroup by a cyclic subgroup of order  $q^n$  ( $G$  is, in fact, a metacyclic group). Now, the proof is completed by the remark that  $T$  can be chosen to be of a prime order  $p$  (we can replace it by a normal subgroup  $T' \leq T$  of order  $p$ ).

Case II. Now assume that  $G$  is a  $p$ -group. Let  $M_1$  be a minimal normal subgroup of  $G$ . If there is  $M_2 \in L(G)$ ,  $M_2 \neq M_1$ , with  $|M_2| = p$ , then  $G$  will

contain the noncyclic subgroup  $M_1 M_2 \cong \mathbb{Z}_p \times \mathbb{Z}_p$ . It follows that  $G = M_1 M_2$  and so  $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ . If  $M_1$  is the unique subgroup of order  $p$  in  $G$ , then, by [6, vol. II, eq. (4.4)],  $G$  is isomorphic to a generalized quaternion group

$$Q_{2^n} = \langle a, b \mid a^{2^{n-2}} = b^2, a^{2^{n-1}} = 1, b^{-1}ab = a^{-1} \rangle, n \geq 3.$$

Let  $H = \langle a^2, b \rangle \cong Q_{2^{n-1}}$ . Clearly,  $H$  is a proper non-cyclic subgroup of  $G$  for  $n \geq 4$ . Hence  $n = 3$ , i.e.,  $G \cong Q_8$ .  $\square$

In what follows assume that  $G$  and  $G'$  are two finite groups. It is obvious that if  $G \cong G'$ , then  $\text{cdeg}(G) = \text{cdeg}(G')$ . In particular, we infer that any two conjugate subgroups of a finite group have the same cyclicity degree. We remark that the above conclusion remains true even in the case when  $G$  and  $G'$  are only lattice-isomorphic ( $L$ -isomorphic), i.e., there is an isomorphism from  $L(G)$  to  $L(G')$ , because lattice-isomorphisms preserve cyclic subgroups by [15, Th. 1.2.10].

By a direct calculation, one obtains

$$\text{cdeg}(S_3 \times \mathbb{Z}_2) = \frac{5}{8} \neq \frac{5}{6} = \text{cdeg}(S_3) \text{cdeg}(\mathbb{Z}_2)$$

and therefore in general we do not have  $\text{cdeg}(G \times G') = \text{cdeg}(G) \text{cdeg}(G')$ . It is clear that a sufficient condition for this equality to hold is

$$\gcd(|G|, |G'|) = 1,$$

that is  $G$  and  $G'$  are of coprime orders. This can be extended to arbitrary finite direct products.

**Proposition 2.2.** *Let  $(G_i)_{1 \leq i \leq k}$  be a family of finite groups having coprime orders. Then*

$$\text{cdeg}\left(\prod_{i=1}^k G_i\right) = \prod_{i=1}^k \text{cdeg}(G_i).$$

The following immediate consequence of Proposition 2.2 shows that computing the cyclicity degree of a finite nilpotent group is reduced to finite  $p$ -groups.

**Corollary 2.3.** *If  $G$  is a finite nilpotent group and  $(G_i)_{1 \leq i \leq k}$  are the Sylow subgroups of  $G$ , then*

$$\text{cdeg}(G) = \prod_{i=1}^k \text{cdeg}(G_i).$$

In order to determine the cyclicity degree of a finite group  $G$  it is essential to find the number of its cyclic subgroups and this is strongly connected with the number of elements of certain orders in  $G$ . For every divisor  $d$  of  $n$  let  $c(d) = |\{H \in C(G) : |H| = d\}|$ . Then

$$|G| = \sum_{d|n} c(d)\varphi(d), \quad (1)$$

where  $\varphi$  is Euler's totient function, and

$$|C(G)| = \sum_{d|n} c(d). \quad (2)$$

In many particular cases the above two identities lead to a precise expression of  $|C(G)|$ . For example, if  $G = \mathbb{Z}_p^k$  is the elementary abelian  $p$ -group of rank  $k$  (that is  $|G| = p^k$ ), then we can easily obtain  $c(1) = 1$ ,  $c(p) = \frac{p^k - 1}{p - 1}$  and  $c(p^2) = c(p^3) = \dots = c(p^k) = 0$ . So,  $|C(\mathbb{Z}_p)| = 2$  and for  $k \geq 2$  we have

$$|C(\mathbb{Z}_p^k)| = 2 + p + p^2 + \dots + p^{k-1}.$$

Furthermore, as it is well known,  $|L(\mathbb{Z}_p^k)| = \sum_{j=0}^k \begin{bmatrix} k \\ j \end{bmatrix}_p$  in terms of the Gaussian coefficients. This can be written in an alternate form, see [20, Prop. 2.12]), giving the following identity for  $\text{cdeg}(\mathbb{Z}_p^k)$ .

**Proposition 2.4.** *The cyclicity degree of the elementary abelian  $p$ -group  $\mathbb{Z}_p^k$  ( $k \geq 2$ ) is given by*

$$\text{cdeg}(\mathbb{Z}_p^k) = \frac{2 + p + p^2 + \dots + p^{k-1}}{2 + \sum_{\alpha=1}^{k-1} \sum_{1 \leq i_1 < i_2 < \dots < i_\alpha \leq k} p^{i_1 + i_2 + \dots + i_\alpha - \frac{\alpha(\alpha+1)}{2}}}.$$

In particular,

$$\text{cdeg}(\mathbb{Z}_p) = 1, \quad \text{cdeg}(\mathbb{Z}_p^2) = \frac{p+2}{p+3}, \quad \text{cdeg}(\mathbb{Z}_p^3) = \frac{1}{2},$$

$$\text{cdeg}(\mathbb{Z}_p^4) = \frac{p^3 + p^2 + p + 2}{p^4 + 3p^3 + 4p^2 + 3p + 5}.$$

Observe that  $\lim_{p \rightarrow \infty} \text{cdeg}(\mathbb{Z}_p^4) = 0$ . This shows the following property.

**Corollary 2.5.**  $\inf\{\text{cdeg}(G) : G \text{ is a finite group}\} = 0$ .

### 3 Cyclicity degrees for some classes of finite groups

In this section we determine explicitly the cyclicity degree of several finite groups. The most significant results are obtained for abelian groups, hamiltonian groups,  $p$ -groups possessing a cyclic maximal subgroup and ZM-groups.

#### 3.1 The cyclicity degree of abelian groups

According to Proposition 2.2, our study can be reduced to finite abelian  $p$ -groups. However, we present first the next result concerning the group  $\mathbb{Z}_m \times \mathbb{Z}_n$ . It was proved in [4, Th. 3 and 5] that for every  $m, n \in \mathbb{N}^*$  the number of cyclic subgroups of  $\mathbb{Z}_m \times \mathbb{Z}_n$  and the total number of its subgroups is given by the identities

$$cs(m, n) := |C(\mathbb{Z}_m \times \mathbb{Z}_n)| = \sum_{a|m, b|n} \varphi(\gcd(a, b)) \quad (3)$$

and

$$s(m, n) := |L(\mathbb{Z}_m \times \mathbb{Z}_n)| = \sum_{a|m, b|n} \gcd(a, b). \quad (4)$$

The identity (4) is a special case of the more general result of [1]. We deduce the following formula.

**Theorem 3.1.1.** *The cyclicity degree of the group  $\mathbb{Z}_m \times \mathbb{Z}_n$  ( $m, n \in \mathbb{N}^*$ ) is*

$$\text{cdeg}(\mathbb{Z}_m \times \mathbb{Z}_n) = \frac{cs(m, n)}{s(m, n)} \quad (5)$$

where  $cs(m, n)$  and  $s(m, n)$  are given by (3) and (4), respectively.

We note that for every  $n_1, \dots, n_k \in \mathbb{N}^*$ ,

$$|C(\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k})| = \sum_{a_1|n_1, \dots, a_k|n_k} \frac{\varphi(a_1) \cdots \varphi(a_k)}{\varphi(\text{lcm}(a_1, \dots, a_k))}, \quad (6)$$

which was proved using the orbit counting lemma (Burnside's lemma) in [26] and by simple number-theoretic arguments in [27].

A formula for  $\text{cdeg}(\mathbb{Z}_m \times \mathbb{Z}_n \times \mathbb{Z}_r)$  ( $m, n, r \in \mathbb{N}^*$ ), which is similar to (5) follows at once from (6) applied for  $k = 3$  and from the identity derived for  $|L(\mathbb{Z}_m \times \mathbb{Z}_n \times \mathbb{Z}_r)|$  in [5, Th. 2.2].

Consider now finite abelian  $p$ -groups. By the fundamental theorem of finitely generated abelian groups, such a group has a direct decomposition of type

$$\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_k}},$$

where  $p$  is a prime and  $1 \leq \alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k$ .

Assume that  $k = 2$ . Then we have the next result.

**Corollary 3.1.2.** *The cyclicity degree of the abelian  $p$ -group  $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$  is given by the following identity:*

$$\begin{aligned} & \text{cdeg}(\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}) \\ &= \frac{(\alpha_2 - \alpha_1 + 1)p^{\alpha_1+2} - 2(\alpha_2 - \alpha_1)p^{\alpha_1+1} + (\alpha_2 - \alpha_1 - 1)p^{\alpha_1} - 2p + 2}{(\alpha_2 - \alpha_1 + 1)p^{\alpha_1+2} - (\alpha_2 - \alpha_1 - 1)p^{\alpha_1+1} - (\alpha_1 + \alpha_2 + 3)p + (\alpha_1 + \alpha_2 + 1)}. \end{aligned}$$

*Proof.* Follows from Theorem 3.1.1 by computing the values of the corresponding sums. Alternatively, one can use the explicit formulas

$$\begin{aligned} |C(\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}})| &= 2 + 2p + \dots + 2p^{\alpha_1-1} + (\alpha_2 - \alpha_1 + 1)p^{\alpha_1}, \\ |L(\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}})| &= \frac{1}{(p-1)^2} ((\alpha_2 - \alpha_1 + 1)p^{\alpha_1+2} - (\alpha_2 - \alpha_1 - 1)p^{\alpha_1+1} - (\alpha_1 + \alpha_2 + 3)p + (\alpha_1 + \alpha_2 + 1)) \end{aligned}$$

obtained in [22, Th. 3.3, 4.2] by different arguments.  $\square$

For an arbitrary  $k$ , a similar formula is more difficult to obtain. It is well-known that  $|L(\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_k}})|$  can recursively be computed. Explicit formulas are known only in certain particular cases, as that in Proposition 2.4. Another example of an explicit formula is that for  $|L(\mathbb{Z}_{p^\alpha} \times \mathbb{Z}_{p^\alpha} \times \mathbb{Z}_{p^\alpha})|$  ( $\alpha \in \mathbb{N}^*$ ), given in [5, Remark 2.1]. At the same time,

$$|C(\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_k}})| = \sum_{\alpha=1}^{\alpha_k} \frac{p^\alpha h_p^{k-1}(\alpha) - p^{\alpha-1} h_p^{k-1}(\alpha-1)}{p^\alpha - p^{\alpha-1}},$$

where

$$h_p^{k-1}(\alpha) = \begin{cases} p^{(k-1)\alpha}, & \text{if } 0 \leq \alpha \leq \alpha_1; \\ p^{(k-2)\alpha + \alpha_1}, & \text{if } \alpha_1 \leq \alpha \leq \alpha_2; \\ \vdots & \\ p^{\alpha_1 + \alpha_2 + \dots + \alpha_{k-1}}, & \text{if } \alpha_{k-1} \leq \alpha \end{cases}$$

(see [22, Th. 4.3]). More precisely, one obtains

$$\begin{aligned} |C(\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \dots \times \mathbb{Z}_{p^{\alpha_k}})| &= 1 + (\alpha_k - \alpha_{k-1})p^{\alpha_1 + \alpha_2 + \dots + \alpha_{k-1}} + \\ &+ \frac{1}{p-1} \sum_{i=1}^{k-1} p^{\alpha_1 + \alpha_2 + \dots + \alpha_{i-1}} \frac{p^{k-i+1}}{p^{k-i}} (p^{(k-i)\alpha_i} - p^{(k-i)\alpha_{i-1}}). \end{aligned}$$

Since the cyclic subgroup structure of a finite group is preserved by  $L$ -isomorphisms, we remark that the above formulas can be used to compute the cyclicity degree of groups which are  $L$ -isomorphic with finite abelian groups. For example, the cyclicity degrees of  $P$ -groups (see [15, Sect. 2.2]) can be found by Proposition 2.4.

We close this subsection with the following properties. According to Proposition 2.2 the function  $n \mapsto f(n) := \text{cdeg}(\mathbb{Z}_n \times \mathbb{Z}_n) \in (0, 1]$  ( $n \in \mathbb{N}^*$ ) is multiplicative, that is  $f(mn) = f(m)f(n)$  for every  $m, n \in \mathbb{N}^*$  with  $\gcd(m, n) = 1$ . Furthermore, by Corollary 3.1.2 for every prime power  $p^\alpha$  ( $\alpha \in \mathbb{N}^*$ ),

$$f(p^\alpha) = \frac{p^{\alpha+2} - p^\alpha - 2p + 2}{p^{\alpha+2} + p^{\alpha+1} - (2\alpha + 3)p + (2\alpha + 1)}.$$

Remark that  $\lim_{p \rightarrow \infty} f(p^\alpha) = 1$  for every fixed  $\alpha \in \mathbb{N}^*$  and  $\lim_{\alpha \rightarrow \infty} f(p^\alpha) = 1 - 1/p$  for every fixed prime  $p$ . Since the series taken over the primes

$$\sum_p \frac{1 - f(p)}{p} = \sum_p \frac{1}{p(p+3)}$$

is convergent, it follows from the theorem of Delange (see, e.g., [13]) that the function  $f$  has a non-zero mean value  $M$  given by

$$M := \lim_{x \rightarrow \infty} \frac{1}{x} \sum_{n \leq x} f(n) = \prod_p \left(1 - \frac{1}{p}\right) \sum_{a=0}^{\infty} \frac{f(p^a)}{p^a},$$

the product being over the primes. Here  $M \approx 0.742$ .

More exactly, the following asymptotic formula holds, for which we give a self contained proof.



**Theorem 3.1.3.**

$$\sum_{n \leq x} \text{cdeg}(\mathbb{Z}_n \times \mathbb{Z}_n) = Mx + O(\log^3 x).$$

*Proof.* Let  $f(n) = \sum_{d|n} g(d)$  ( $n \in \mathbb{N}^*$ ), that is  $g = \mu * f$  in terms of the Dirichlet convolution, where  $\mu$  is the Möbius function. Here  $g(p^a) = f(p^a) - f(p^{a-1})$  ( $a \in \mathbb{N}^*$ ), in particular,

$$g(p) = -\frac{1}{p+3}, \quad g(p^2) = -\frac{3p+4}{(p+3)(p^2+3p+5)}.$$

It follows that  $|g(p)| < \frac{1}{p}$ ,  $|g(p^2)| < \frac{3}{p^2}$  for every prime  $p$ , and direct computations show that  $|g(p^a)| < \frac{2a-1}{p^a}$  for every prime power  $p^a$  ( $a \in \mathbb{N}^*$ ). Hence,  $|g(n)| \leq \tau(n^2)/n$  for every  $n \in \mathbb{N}^*$ , where  $\tau(k)$  stands for the number of positive divisors of  $k$ .

Now,

$$\begin{aligned} \sum_{n \leq x} f(n) &= \sum_{de \leq x} g(d) = \sum_{d \leq x} \sum_{e \leq x/d} 1 = \sum_{d \leq x} (x/d + O(1)) \\ &= x \sum_{d=1}^{\infty} \frac{g(d)}{d} + O\left(x \sum_{d > x} \frac{|g(d)|}{d}\right) + O\left(\sum_{d \leq x} |g(d)|\right) \\ &= Mx + O\left(x \sum_{d > x} \frac{\tau(d^2)}{d^2}\right) + O\left(\sum_{d \leq x} \frac{\tau(d^2)}{d}\right), \end{aligned}$$

where in the main term the coefficient of  $x$  is  $M$  by the Euler's product formula. It is known that  $\sum_{n \leq x} \tau(n^2) = cx \log^2 x + O(x \log x)$  with a certain constant  $c$  and partial summation shows that  $\sum_{n > x} \tau(n^2)/n^2 = O((\log^2 x)/x)$ ,  $\sum_{n \leq x} \tau(n^2)/n = O(\log^3 x)$ .  $\square$

## 3.2 The cyclicity degree of hamiltonian groups

An important class of finite groups which are closely connected to abelian groups consists of hamiltonian groups, that is nonabelian groups all of whose subgroups are normal. The structure of such a group  $H$  is well-known, namely

$$H \cong Q_8 \times \mathbb{Z}_2^n \times A$$

where  $A$  is an abelian group of odd order. By Proposition 2.2 we infer that

$$\text{cdeg}(H) = \text{cdeg}(Q_8 \times \mathbb{Z}_2^n) \text{cdeg}(A),$$

which shows that the computation of  $\text{cdeg}(H)$  is reduced to the computation of  $\text{cdeg}(Q_8 \times \mathbb{Z}_2^n)$ . The number of subgroups of  $Q_8 \times \mathbb{Z}_2^n$  has been determined in [24]:

$$|L(Q_8 \times \mathbb{Z}_2^n)| = b_{n,2} = 2^{n+2} + 1 + 8 \sum_{\alpha=0}^{n-2} (2^{n-\alpha} - 2^{2\alpha+1} + 2^\alpha) a_{\alpha,2} + 2^{n+2} a_{n-1,2} + a_{n,2},$$

where  $a_{\alpha,2} = |L(\mathbb{Z}_2^\alpha)|$ , for all  $\alpha \in \mathbb{N}^*$ . Moreover, the equalities (1) and (2) become in this case

$$2^{n+3} = \sum_{d|2^{n+3}} c(d) \varphi(d) \quad \text{and} \quad |C(Q_8 \times \mathbb{Z}_2^n)| = \sum_{d|2^{n+3}} c(d),$$

respectively. Since  $c(1) = 1$  and  $c(2^i) = 0$ , for all  $i \geq 3$ , one obtains

$$2^{n+3} = 1 + c(2) + 2c(4) \quad \text{and} \quad |C(Q_8 \times \mathbb{Z}_2^n)| = 1 + c(2) + c(4).$$

These show that

$$|C(Q_8 \times \mathbb{Z}_2^n)| = 2^{n+3} - c(4).$$

Clearly, the cyclic subgroups of order 4 of  $Q_8 \times \mathbb{Z}_2^n$  are of type  $\langle (x, y) \rangle$ , where  $x \in Q_8$  has order 4 and  $y \in \mathbb{Z}_2^n$  is arbitrary. We infer that  $c(4) = 3 \cdot 2^n$  and so

$$|C(Q_8 \times \mathbb{Z}_2^n)| = 5 \cdot 2^n.$$

Hence we have proved the following result.

**Theorem 3.2.1.** *The cyclicity degree of the hamiltonian group  $H \cong Q_8 \times \mathbb{Z}_2^n \times A$  is given by the following equality:*

$$\text{cdeg}(H) = \frac{5 \cdot 2^n}{b_{n,2}} \text{cdeg}(A).$$

### 3.3 The cyclicity degree of finite $p$ -groups possessing a cyclic maximal subgroup

Let  $p$  be a prime,  $n \geq 3$  be an integer and denote by  $\mathcal{G}$  the class consisting of all finite  $p$ -groups of order  $p^n$  having a maximal subgroup which is cyclic. Obviously,  $\mathcal{G}$  contains the finite abelian  $p$ -groups of type  $\mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}$  whose cyclicity degrees have been computed in Section 3.1, but some finite nonabelian  $p$ -groups belong to  $\mathcal{G}$ , too. They are exhaustively described in [17, Vol. II, Th. 4.1]: a nonabelian group is contained in  $\mathcal{G}$  if and only if it is isomorphic to

$$- M(p^n) = \langle x, y \mid x^{p^{n-1}} = y^p = 1, y^{-1}xy = x^{p^{n-2}+1} \rangle$$

when  $p$  is odd, or to one of the following groups

- $M(2^n)$  ( $n \geq 4$ ),
- the dihedral group  $D_{2^n}$ ,
- the generalized quaternion group

$$Q_{2^n} = \langle x, y \mid x^{2^{n-1}} = y^4 = 1, yxy^{-1} = x^{2^{n-1}-1} \rangle,$$

- the quasi-dihedral group

$$S_{2^n} = \langle x, y \mid x^{2^{n-1}} = y^2 = 1, y^{-1}xy = x^{2^{n-2}-1} \rangle \quad (n \geq 4)$$

when  $p = 2$ .

In the following the cyclicity degrees of the above  $p$ -groups will be determined. We recall first the explicit formulas for the total number of subgroups of these groups (see [23, Lemma 3.2.1]).

**Lemma 3.3.1.** *The following equalities hold:*

- a)  $|L(M(p^n))| = (1+p)n + 1 - p$ ,
- b)  $|L(D_{2^n})| = 2^n + n - 1$ ,
- c)  $|L(Q_{2^n})| = 2^{n-1} + n - 1$ ,
- d)  $|L(S_{2^n})| = 3 \cdot 2^{n-2} + n - 1$ .

Computing the cyclic subgroups of groups in  $\mathcal{G}$  is facile by using their maximal subgroup structure and the well-known Inclusion-Exclusion Principle (IEP, in short).

$M(p^n)$  has  $p + 1$  maximal subgroups:  $M_0 = \langle x \rangle$ ,  $M_1 = \langle xy \rangle$ , ...,  $M_{p-1} = \langle x^{p-1}y \rangle$  and  $M_p = \langle x^p, y \rangle$ . Moreover,  $M_i \cong \mathbb{Z}_{p^{n-1}}$ , for  $i = 0, 1, \dots, p-1$ ,  $M_p = \langle x^p, y \rangle \cong \mathbb{Z}_{p^{n-2}} \times \mathbb{Z}_p$  and any intersection of at least two distinct such subgroups is isomorphic to  $\mathbb{Z}_{p^{n-2}}$ . We infer that

$$\begin{aligned}
|C(M(p^n))| &= \left| \bigcup_{i=0}^p C(M_i) \right| = \\
&= \sum_{i=0}^p |C(M_i)| - \sum_{0 \leq i_1 < i_2 \leq p} |C(M_{i_1} \cap M_{i_2})| + \dots + (-1)^p \left| \bigcap_{i=0}^p C(M_i) \right| = \\
&= p |C(\mathbb{Z}_{p^{n-1}})| + |C(\mathbb{Z}_{p^{n-2}} \times \mathbb{Z}_p)| - |C(\mathbb{Z}_{p^{n-2}})| \sum_{i=2}^{p+1} (-1)^i \binom{p+1}{i} = \\
&= np + (n-2)p + 2 - (n-1)p = (n-1)p + 2,
\end{aligned}$$

which leads to the following theorem.

**Theorem 3.3.2.** *The cyclicity degree of  $M(p^n)$  is*

$$\text{cdeg}(M(p^n)) = \frac{(n-1)p + 2}{(n-1)p + n + 1}.$$

**Corollary 3.3.3.** *We have:*

- a)  $\lim_{n \rightarrow \infty} \text{cdeg}(M(p^n)) = \frac{p}{p+1}$ , for every fixed prime  $p$ .
- b)  $\lim_{p \rightarrow \infty} \text{cdeg}(M(p^n)) = 1$ .

The group  $D_{2^n}$  has 3 maximal subgroups:  $M_0 = \langle x \rangle \cong \mathbb{Z}_{2^{n-1}}$ ,  $M_1 = \langle x^2, y \rangle \cong D_{2^{n-1}}$  and  $M_2 = \langle x^2, xy \rangle \cong D_{2^{n-1}}$ . By applying IEP, one obtains the recurrence relation

$$|C(D_{2^n})| = 2|C(D_{2^{n-1}})| + 2 - n,$$

which implies that

$$|C(D_{2^n})| = 2^{n-1} + n.$$

So, we have:

**Theorem 3.3.4.** *The cyclicity degree of  $D_{2^n}$  is*

$$\text{cdeg}(D_{2^n}) = \frac{2^{n-1} + n}{2^n + n - 1}.$$

**Corollary 3.3.5.**  $\lim_{n \rightarrow \infty} \text{cdeg}(D_{2^n}) = \frac{1}{2}.$

$Q_{2^n}$  has 3 maximal subgroups:  $M_0 \cong \mathbb{Z}_{2^{n-1}}$  and  $M_1, M_2 \cong Q_{2^{n-1}}$ . By applying again IEP, we find the following recurrence relation

$$|C(Q_{2^n})| = 2|C(Q_{2^{n-1}})| + 2 - n,$$

proving that

$$|C(Q_{2^n})| = 2^{n-2} + n.$$

In this way, one obtains:

**Theorem 3.3.6.** *The cyclicity degree of  $Q_{2^n}$  is*

$$\text{cdeg}(Q_{2^n}) = \frac{2^{n-2} + n}{2^{n-1} + n - 1}.$$

**Corollary 3.3.7.**  $\lim_{n \rightarrow \infty} \text{cdeg}(Q_{2^n}) = \frac{1}{2}.$

$S_{2^n}$  has 3 maximal subgroups:  $M_0 \cong \mathbb{Z}_{2^{n-1}}$ ,  $M_1 \cong D_{2^{n-1}}$  and  $M_2 \cong Q_{2^{n-1}}$ . In this case IEP leads directly to an explicit formula for the number of cyclic subgroups of  $S_{2^n}$ , namely

$$\begin{aligned} |C(S_{2^n})| &= |C(\mathbb{Z}_{2^{n-1}})| + |C(D_{2^{n-1}})| + |C(Q_{2^{n-1}})| - 2|C(\mathbb{Z}_{2^{n-2}})| = \\ &= 3 \cdot 2^{n-3} + n. \end{aligned}$$

So, we get the following theorem.

**Theorem 3.3.8.** *The cyclicity degree of  $S_{2^n}$  is*

$$\text{cdeg}(S_{2^n}) = \frac{3 \cdot 2^{n-3} + n}{3 \cdot 2^{n-2} + n - 1}.$$

**Corollary 3.3.9.**  $\lim_{n \rightarrow \infty} \text{cdeg}(S_{2^n}) = \frac{1}{2}.$

We end this subsection by observing that the cyclicity degree of any finite nilpotent group whose Sylow subgroups belong to  $\mathcal{G}$  can explicitly be calculated, in view of Corollary 2.3.

### 3.4 The cyclicity degree of ZM-groups

Recall that a ZM-group is a finite group all of whose Sylow subgroups are cyclic. By [6] such a group is of type

$$\text{ZM}(m, n, r) = \langle a, b \mid a^m = b^n = 1, b^{-1}ab = a^r \rangle,$$

where the triple  $(m, n, r)$  satisfies the conditions

$$\gcd(m, n) = \gcd(m, r - 1) = 1 \quad \text{and} \quad r^n \equiv 1 \pmod{m}.$$

It is clear that  $|\text{ZM}(m, n, r)| = mn$ ,  $\text{ZM}(m, n, r)' = \langle a \rangle$  (therefore we have  $|\text{ZM}(m, n, r)'| = m$ ) and  $\text{ZM}(m, n, r)/\text{ZM}(m, n, r)'$  is cyclic of order  $n$ . The subgroups of  $\text{ZM}(m, n, r)$  have been completely described in [1]. Set

$$L = \left\{ (m_1, n_1, s) \in \mathbb{N}^{*2} \times \mathbb{N} : m_1 \mid m, n_1 \mid n, 0 \leq s \leq m_1 - 1, m_1 \mid s \frac{r^n - 1}{r^{n_1} - 1} \right\}.$$

Then there is a bijection between  $L$  and the subgroup lattice  $L(\text{ZM}(m, n, r))$  of  $\text{ZM}(m, n, r)$ , namely the function that maps a triple  $(m_1, n_1, s) \in L$  into the subgroup  $H_{(m_1, n_1, s)}$  defined by

$$H_{(m_1, n_1, s)} = \bigcup_{k=1}^{\frac{n}{n_1}} \alpha(n_1, s)^k \langle a^{m_1} \rangle = \langle a^{m_1}, \alpha(n_1, s) \rangle,$$

where  $\alpha(x, y) = b^x a^y$ , for all  $0 \leq x < n$  and  $0 \leq y < m$ . Notice that we have

$$|L(\text{ZM}(m, n, r))| = |L| = \sum_{m_1 \mid m} \sum_{n_1 \mid n} \gcd \left( m_1, \frac{r^n - 1}{r^{n_1} - 1} \right). \quad (7)$$

On the other hand, we easily infer that a subgroup  $H_{(m_1, n_1, s)} \in L(\text{ZM}(m, n, r))$  is cyclic if and only if  $\frac{m}{m_1} \mid r^{n_1} - 1$ . This shows that

$$C(\text{ZM}(m, n, r)) = \{ H_{(m_1, n_1, s)} \in L(\text{ZM}(m, n, r)) : (m_1, n_1, s) \in L' \},$$

where

$$L' = \left\{ (m_1, n_1, s) \in L : \frac{m}{m_1} \mid r^{n_1} - 1 \right\}.$$

Hence

$$|C(\text{ZM}(m, n, r))| = |L'| = \sum_{m_1|m} \sum_{\substack{n_1|n \\ m/m_1|r^{n_1}-1}} \gcd\left(m_1, \frac{r^n - 1}{r^{n_1} - 1}\right) \quad (8)$$

and the following result holds.

**Theorem 3.4.1.** *The cyclicity degree of the ZM-group  $\text{ZM}(m, n, r)$  is*

$$\text{cdeg}(\text{ZM}(m, n, r)) = \frac{|L'|}{|L|},$$

where  $|L'|$  and  $|L|$  are given by the identities (8) and (7), respectively.

Simple explicit formulas for  $\text{cdeg}(\text{ZM}(m, n, r))$  can be given in several particular cases. One of them is obtained by taking  $n = 2$ ,  $m \equiv 1 \pmod{2}$  and  $r = -1$ , that is for the dihedral group  $D_{2m}$ . Then it is easy to see that (8) and (7) reduce to

$$|C(D_{2m})| = m + \tau(m),$$

and

$$|L(D_{2m})| = \tau(m) + \sigma(m),$$

where  $\tau(m)$  and  $\sigma(m)$  denote the number and the sum of all divisors of  $m$ , respectively. These formulas are known, they hold true also for  $m$  even and can be proved by a direct counting of the subgroups of  $D_{2m}$ . We obtain the following corollary.

**Corollary 3.4.2.** *The cyclicity degree of the dihedral group  $D_{2m}$  ( $m \in \mathbb{N}^*$ ) is given by the identity*

$$\text{cdeg}(D_{2m}) = \frac{m + \tau(m)}{\tau(m) + \sigma(m)}.$$

**Remark.** The above formula remains true for arbitrary primes  $n$ , not only for  $n = 2$ .

## 4 Some minimality/maximality results on cyclicity degrees

As we already have seen, computing cyclic subgroups and cyclicity degrees of abelian groups is reduced to abelian  $p$ -groups. In this section we are interested to study when for an abelian  $p$ -group  $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_k}}$  ( $\alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k$ ) of a given order  $p^n$  (that is,  $\sum_{i=1}^k \alpha_i = n$ ) the number of cyclic subgroups and the cyclicity degree are minimal/maximal.

We suppose first that  $k = 2$ . Then we have (cf. Section 3.1)

$$\begin{aligned} |C(\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}})| &= 2 + 2p + \dots + 2p^{\alpha_1-1} + (\alpha_2 - \alpha_1 + 1)p^{\alpha_1} = \\ &= 2 + 2p + \dots + 2p^{\alpha_1-1} + (n - 2\alpha_1 + 1)p^{\alpha_1}, \end{aligned}$$

in view of the equality  $\alpha_1 + \alpha_2 = n$ . By studying the above expression as a function in  $\alpha_1$ , we easily infer that it is strictly increasing. Therefore  $|C(\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}})|$  is minimal for  $\alpha_1 = 1$  and maximal for  $\alpha_1 = \lfloor n/2 \rfloor$  (in other words,  $\alpha_1$  and  $\alpha_2$  tend to be equal).

In order to study the cyclicity degree of  $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ , we remark that the formula in Theorem 3.1.1 can be rewritten as

$$\begin{aligned} \text{cdeg}(\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}) &= \\ &= 1 - \frac{1}{p} \left[ 1 - \frac{(\alpha_1 + \alpha_2 + 1)p^2 - 2(\alpha_1 + \alpha_2 + 2)p + (\alpha_1 + \alpha_2 + 1)}{(\alpha_2 - \alpha_1 + 1)p^{\alpha_1+2} - (\alpha_2 - \alpha_1 - 1)p^{\alpha_1+1} - (\alpha_1 + \alpha_2 + 3)p + (\alpha_1 + \alpha_2 + 1)} \right] = \\ &= 1 - \frac{1}{p} \left[ 1 - \frac{(n+1)p^2 - 2(n+2)p + (n+1)}{(n-2\alpha_1+1)p^{\alpha_1+2} - (n-2\alpha_1-1)p^{\alpha_1+1} - (n+3)p + (n+1)} \right]. \end{aligned}$$

The last expression is in this case a strictly decreasing function in  $\alpha_1$ , which shows that  $\text{cdeg}(\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}})$  is minimal for  $\alpha_1 = \lfloor n/2 \rfloor$  and maximal for  $\alpha_1 = 1$ . Hence we have proved the following theorem.

**Theorem 4.1.** *In the class of abelian  $p$ -groups  $G$  of rank 2 and order  $p^n$ , we have that:*

- a)  $|C(G)|$  is minimal (maximal) if and only if  $G \cong \mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}$  (respectively  $G \cong \mathbb{Z}_{p^{\lfloor n/2 \rfloor}} \times \mathbb{Z}_{p^{n-\lfloor n/2 \rfloor}}$ );



- b)  $\text{cdeg}(G)$  is minimal (maximal) if and only if  $G \cong \mathbb{Z}_{p^{\lfloor n/2 \rfloor}} \times \mathbb{Z}_{p^{n-\lfloor n/2 \rfloor}}$  (respectively  $G \cong \mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}$ ).

**Remark.** The above expression also shows that the cyclicity degree of an abelian  $p$ -groups of rank 2 and fixed order depends only on its number of subgroups.

## 5 Further research

Several questions and conjectures on cyclicity degrees of finite groups can be formulated. As an example we give the following

**Problem.** Is it true the following density result on cyclicity degrees: for every  $a \in [0, 1]$  there exists a sequence  $(G_n)_{n \in \mathbb{N}}$  of finite groups such that  $\lim_{n \rightarrow \infty} \text{cdeg}(G_n) = a$ ? Also, is it true that for every  $a \in (0, 1] \cap \mathbb{Q}$  there exists a finite group  $G$  such that  $\text{cdeg}(G) = a$ ?

## References

- [1] Calhoun, W.C., *Counting subgroups of some finite groups*, Amer. Math. Monthly, **94** (1987), 54–59.
- [2] Grätzer, G. *General lattice theory*, Academic Press (New York, 1978).
- [3] Gustafson, W. H., *What is the probability that two group elements commute?*, Amer. Math. Monthly, **80** (1973), 1031–1034.
- [4] Hampejs, M., Holighaus, N., Tóth, L., and Wiesmeyr, C., *Representing and counting the subgroups of the group  $\mathbb{Z}_m \times \mathbb{Z}_n$* , Journal of Numbers, vol. 2014, Article ID 491428, arXiv:1211.1797 [math.GR].
- [5] Hampejs, M. and Tóth, L., *On the subgroups of finite Abelian groups of rank three*, Annales Univ. Sci. Budapest., Sect. Comp., **39** (2013), 111–124.
- [6] Huppert, B., *Endliche Gruppen*, I, II, Springer Verlag (Berlin, 1967, 1968).

- [7] Isaacs, I.M., *Finite group theory*, Amer. Math. Soc. (Providence, RI, 2008).
- [8] Lescot, P., *Sur certains groupes finis*, Rev. Math. Spéciales, **8** (1987), 276–277.
- [9] Lescot, P., *Degré de commutativité et structure d'un groupe fini* (1), Rev. Math. Spéciales, **8** (1988), 276–279.
- [10] Lescot, P., *Degré de commutativité et structure d'un groupe fini* (2), Rev. Math. Spéciales, **4** (1989), 200–202.
- [11] Lescot, P., *Isoclinism classes and commutativity degrees of finite groups*, J. Algebra, **177** (1995), 847–869.
- [12] Lescot, P., *Central extensions and commutativity degree*, Comm. Algebra, **29** (2001), 4451–4460.
- [13] Postnikov, A. G., *Introduction to Analytic Number Theory*, Translations of Mathematical Monographs, 68, Amer. Math. Society (Providence, RI, 1988).
- [14] Rusin, D. J., *What is the probability that two elements of a finite group commute?*, Pacific J. Math., **82** (1979), 237–247.
- [15] Schmidt, R., *Subgroup lattices of groups*, de Gruyter Expositions in Mathematics 14, de Gruyter (Berlin, 1994).
- [16] Sherman, G., *What is the probability an automorphism fixes a group element?*, Amer. Math. Monthly, **82** (1975), 261–264.
- [17] Suzuki, M., *Group theory*, I, II, Springer Verlag (Berlin, 1982, 1986).
- [18] Tărnăuceanu, M., *Actions of finite groups on lattices*, Seminar Series in Mathematics, Algebra 4, Univ. "Ovidius", Constanța, 2003.
- [19] Tărnăuceanu, M., *Groups determined by posets of subgroups*, Ed. Matrix Rom (București, 2006).
- [20] Tărnăuceanu, M., *A new method of proving some classical theorems of abelian groups*, Southeast Asian Bull. Math., **31** (2007), 1191–1203.

- [21] Tărnăuceanu, M., *Subgroup commutativity degrees of finite groups*, J. Algebra, **321** (2009), 2508–2520, doi: 10.1016/j.jalgebra.2009.02.010.
- [22] Tărnăuceanu, M., *An arithmetic method of counting the subgroups of a finite abelian group*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.), **53/101** (2010), 373–386.
- [23] Tărnăuceanu, M., *Addendum to "Subgroup commutativity degrees of finite groups"*, J. Algebra, **337** (2011), 363–368, doi: 10.1016/j.jalgebra.2011.05.001.
- [24] Tărnăuceanu, M., *Some combinatorial aspects of finite Hamiltonian groups*, Bull. Iranian Math. Soc., **39** (2013), 841–854.
- [25] Tărnăuceanu, M., *Normality degrees of finite groups*, submitted.
- [26] Tóth, L., *Menon's identity and arithmetical sums representing functions of several variables*, Rend. Sem. Mat. Univ. Politec. Torino, **69** (2011), 97–110.
- [27] Tóth, L., *On the number of cyclic subgroups of a finite Abelian group*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.), **55(103)** (2012), 423–428.

Marius Tărnăuceanu  
 Faculty of Mathematics  
 "Al.I. Cuza" University  
 Iași, Romania  
 e-mail: `tarnauc@uaic.ro`

László Tóth  
 Department of Mathematics  
 University of Pécs  
 Pécs, Hungary  
 e-mail: `ltoth@gamma.ttk.pte.hu`